Jak chronić Zarząd, majątek i ciągłość działania spółdzielni przed współczesnymi zagrożeniami

CEL I ZAŁOŻENIA KONFERENCJI

Żaden przepis nie wymaga od członka Zarządu, aby sam konfigurował serwery, wykonywał kopie zapasowe czy analizował logi systemowe. Wymaga natomiast, aby zapewnił właściwą organizację bezpieczeństwa, wyznaczył odpowiedzialne osoby, sprawował nadzór nad realizacją obowiązków oraz podejmował świadome decyzje dotyczące bezpieczeństwa spółdzielni.

Celem konferencji jest pokazanie, jak skutecznie zarządzać bezpieczeństwem spółdzielni, aby chronić jej majątek, dane i ciągłość działania, a jednocześnie wykazać należytą staranność oraz ograniczyć ryzyko odpowiedzialności członków Zarządu.

Konferencja oparta została na analizie rzeczywistych zdarzeń oraz praktycznych przykładach, które pokażą, jak organizować system bezpieczeństwa, budować odporność organizacji na współczesne zagrożenia oraz wdrażać rozwiązania skutecznie chroniące spółdzielnię i ograniczające ryzyko odpowiedzialności członków Zarządu.

DZIEŃ I

Współczesne zagrożenia dla spółdzielni – cyberbezpieczeństwo, oszustwa i sztuczna inteligencja

1. **Dlaczego Zarządy są celem współczesnych ataków**
   (aktualne zagrożenia, metody działania cyberprzestępców, ataki ukierunkowane na osoby zarządzające)
2. **Najczęstsze scenariusze cyberataków i oszustw**
   (phishing, ransomware, przejęcie poczty elektronicznej, oszustwa finansowe, wyciek danych, deepfake)
3. **Sztuczna inteligencja – nowe możliwości i nowe zagrożenia**
   (wykorzystanie AI przez cyberprzestępców, bezpieczne korzystanie z narzędzi AI, dobre praktyki)
4. **Jak reagować na incydent bezpieczeństwa**
   (pierwsze działania po incydencie, ograniczanie skutków, współpraca z działem IT i Inspektorem Ochrony Danych)

Jak Zarząd skutecznie organizuje bezpieczeństwo spółdzielni i ogranicza ryzyko odpowiedzialności członków Zarządu?

1. **Bezpieczeństwo spółdzielni jako element zarządzania organizacją**
   (rola Zarządu w tworzeniu systemu bezpieczeństwa, wyznaczanie odpowiedzialnych osób, nadzór nad realizacją obowiązków, podejmowanie świadomych decyzji dotyczących bezpieczeństwa spółdzielni)
2. **Organizacja systemu bezpieczeństwa – współpraca Zarządu ze specjalistami**
   (współpraca z działem IT, Inspektorem Ochrony Danych i podmiotami zewnętrznymi, określanie zakresów odpowiedzialności, skuteczny nadzór nad powierzonymi zadaniami, weryfikowanie realizacji obowiązków)
3. **Zarządzanie ryzykiem i przygotowanie spółdzielni na sytuacje kryzysowe**
   (identyfikowanie najważniejszych zagrożeń, analiza ryzyka, procedury reagowania, plan ciągłości działania, kopie zapasowe, przygotowanie organizacji do funkcjonowania po incydencie)

4. **Ochrona danych osobowych jako część systemu bezpieczeństwa spółdzielni**
   (RODO jako narzędzie porządkowania procesów, dokumentowanie działań, wykazywanie należytej staranności, współpraca Zarządu z Inspektorem Ochrony Danych)
5. **Jak wykazać należytą staranność i ograniczyć ryzyko odpowiedzialności członków Zarządu**
   (dokumentowanie decyzji i działań, reagowanie na sygnały o zagrożeniach, nadzorowanie wdrożonych rozwiązań, okresowa weryfikacja systemu bezpieczeństwa)

DZIEŃ II

Warsztat dla Zarządów

Bezpieczny Zarząd – rozmowa o bezpieczeństwie spółdzielni

Drugi dzień konferencji będzie miał formę warsztatową i będzie poświęcony praktycznym aspektom zarządzania bezpieczeństwem w spółdzielni mieszkaniowej. Uczestnicy będą mieli możliwość omówienia rzeczywistych problemów, wymiany doświadczeń oraz zadawania pytań ekspertom.

Zakres warsztatu

1. Jak ocenić poziom bezpieczeństwa swojej spółdzielni

- najważniejsze obszary wpływające na bezpieczeństwo organizacji,
- sygnały ostrzegawcze,
- najczęściej występujące problemy organizacyjne.

2. Analiza rzeczywistych przypadków

- przykłady incydentów w organizacjach,
- omówienie przyczyn i konsekwencji,
- dyskusja nad rozwiązaniami.

3. Panel pytań i odpowiedzi

- odpowiedzi ekspertów na pytania uczestników,
- wymiana doświadczeń pomiędzy Zarządami.